УДК 681.3, 004.932.2
doi:10.15217/issn1684-8853.2017.6.88

МАСКИРУЮЩЕЕ СЖАТИЕ НА ОСНОВЕ МОДЕЛИ ВЗВЕШЕННОЙ СТРУКТУРЫ ИЗОБРАЖЕНИЯ

С. В. Беззатеев[a]***,*** *доктор техн. наук, доцент*
Н. В. Волошина[a]***,*** *канд. техн. наук, доцент*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*

Введение: *для организации эффективного и безопасного хранения и передачи видеоинформации необходимо использовать две независимые и последовательные процедуры — сжатие и маскирование. При получении информации на принимающей стороне следует выполнить операции декомпрессии и дешифрации в обратном порядке, чтобы получить исходное изображение. Для выполнения процедуры декомпрессии надо иметь так называемую «кодовую книгу» аналогично ключу в процедурах шифрования и дешифрации.* ***Цель исследования:*** *разработка эффективного способа объединения процедур сжатия и маскирования для цифровых изображений.* ***Результаты:*** *предложен метод сжатия, учитывающий значимости различных частей исходного мультимедийного объекта (изображения) для повышения качества результирующего изображения после декомпрессии. Одним из наиболее эффективных подходов для разработки такого метода сжатия является использование кодов, корректирующих ошибки и позволяющих ограничить число возникающих ошибок (искажений), а также обеспечить требуемое значение коэффициента сжатия. Применение таких кодов для сжатия дает возможность распределять ошибки, которые добавляются в процессе обработки, в соответствии с предустановленной значимостью исходных элементов мультимедийного объекта. В качестве примера представлен подход, основанный на взвешенной метрике Хэмминга, гарантирующий заданное максимальное число ошибок (искажений) и учитывающий предустановленную значимость зон изображения (взвешенную структуру изображения). Для реализации предложенного метода совместного маскирования и сжатия был выбран подкласс кодов Гоппы, совершенных во взвешенной метрике Хэмминга, при этом многочлены Гоппы использовались в качестве секретного ключа. Результатом использования предложенного метода совместного маскирования и сжатия является покрытие всего изображения уникальным цифровым водяным знаком.* ***Практическая значимость:*** *практическое использование предлагаемого подхода возможно в системах с повышенными требованиями по качеству хранимых и передаваемых изображений при использовании открытых каналов передачи для обеспечения как гарантированного эффекта сжатия при заданном уровне вносимых искажений, так и защиты информации.*

Ключевые слова *— кодовое квантование, совершенные коды, взвешенная метрика расстояния, стеганография.*

Введение

В современных киберфизических системах непрерывно хранится, обрабатывается и передается большое число мультимедийных данных [1]. Информация такого типа отличается большим объемом и избыточностью, поэтому требует предварительной обработки — сжатия для эффективного использования каналов связи и памяти [2, 3]. В связи с тем, что в современных информационно-коммуникационных системах активно используются распределенные хранилища данных и открытые каналы связи, необходимо защищать хранящуюся и передаваемую информацию от несанкционированного доступа. Во многих случаях такая защита может требовать не полной недоступности информации, а лишь значительного ухудшения качества, например, для изображений в случае, когда не известен секретный ключ [4]. При этом информация может быть распознаваемой, но не пригодной для коммерческого использования. Для решения подобного типа задач можно использовать подход кодового квантования изображений на кодах Гоппы, совершенных во взвешенной метрике Хэмминга.

Декомпозиция исходного изображения на блоки с длиной K и замена этих блоков на блоки с меньшей длиной k является очень эффективным методом преобразования изображений, например, для сжатия с потерями или установки цифрового водяного знака [5, 6]. Для реализации такого подхода необходимо изначально определить соответствующее правило, устанавливающее соотношение между исходным и результирующим блоками. Следует заметить, что если несколько блоков исходного изображения заменяются одним и тем же блоком результирующего изображения (так называемым сурьективным отображением), то это приводит к появлению ошибок в результирующем изображении, которые визуально могут проявляться как искажения исходного изображения.

Кодовое сжатие изображений

Рассмотрим процедуру сжатия в качестве основы для построения системы эффективного хранения и передачи мультимедиаинформации в открытых и распределенных системах. При использовании сжатия для изображений должны быть определены следующие параметры:

— коэффициент сжатия Θ;

— коэффициент вносимых искажений ρ.

В данной работе для определенности будем считать, что число различных значений блока K равно N. Например, пусть блок исходного изображения состоит из m пикселей, а каждый пиксель состоит из n бит. Тогда $N = 2^{mn}$ и блок исходного изображения представлен в виде двоичного кода длиной $K = mn$.

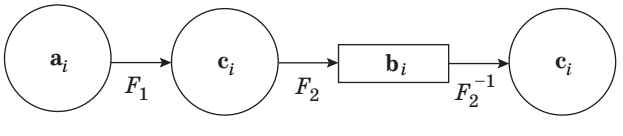
Для простоты рассмотрения, но без потери общности будем использовать один из самых простых форматов представления изображений — формат .bmp. Пусть для данного формата размер блока исходного изображения определен как 8×8, т. е. состоящий из $m = 64$ пикселей. Для цветных изображений, например RGB, число бит на один пиксель может быть определено как $n = 8\times3 = 24$ и, соответственно, $K = m\times n = 64\times24 = 1536$. В этом случае $N = 2^{1536}$. В то же время при независимом покомпонентном сжатии $N = 2^{64\times8} = 2^{512}$. Таким образом, длина блока исходного изображения определяется для каждого случая отдельно и может иметь различные значения.

Далее определим M как общее число различных значений для блоков результирующего изображения, полученного в итоге выполнения процедуры сжатия. Тогда после завершения процедуры сжатия для каждого блока исходного изображения мы получим блок результирующего изображения в виде двоичного вектора длины $k = \log_2 M$.

В этом случае коэффициент сжатия может быть определен как $\Theta = K/k$.

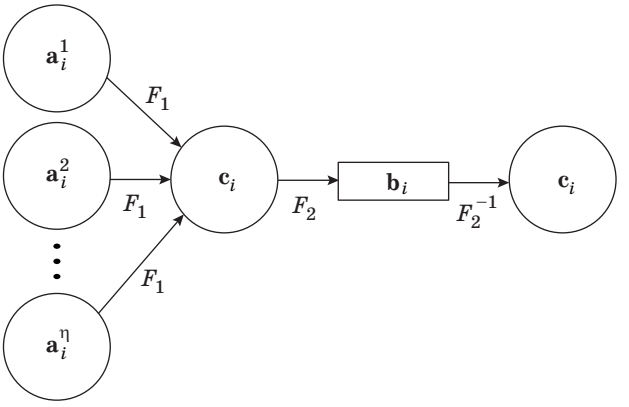
На рис. 1 представлена схема процедуры кодового сжатия, при которой происходит отображение блока исходного изображения $\mathbf{a}_i$ длины K в блок сжатого изображения (файла) $\mathbf{b}_i$ длины k с дальнейшей декомпрессией в блок результирующего изображения $\mathbf{c}_i$, где F_1 — функция кодирования; F_2 — функция построения кодовой книги; F_2^{-1} — функция декодирования. Важно отметить, что для правильного декодирования необходимо использовать тот же помехоустойчивый код, который был использован для процедур F_1 и F_2.

Поскольку при кодировании в целях осуществления сжатия (кодового квантования) $M < N$, то может существовать $\eta = \dfrac{N}{M}$ различных блоков исходного изображения $\left\{\mathbf{a}_i^1, \mathbf{a}_i^2, \ldots, \mathbf{a}_i^\eta\right\}$, преобразуемых в результате кодового квантования в один и тот же блок результирующего изображения $\mathbf{c}_i$. Схематично сурьективное отображение блоков исходного изображения в блоки проквантованного (сжатого) изображения показано на рис. 2.



■ ***Рис. 1.*** Схема процедур кодового сжатия и восстановления

■ ***Fig. 1.*** Code based image compression/decompression procedure scheme



■ ***Рис. 2.*** Сурьективное отображение блоков исходного изображения при кодовом сжатии

■ ***Fig. 2.*** Initial block to resulting compressed block mapping

Такое отображение может приводить к возникновению ошибок квантования и, как следствие, к появлению искажений в результирующем (восстановленном) изображении и тем самым к ухудшению его качества. Для оценки искажений, возникающих в процессе сжатия-восстановления, определим расстояние между исходным $\mathbf{a}_i$ и восстановленным после сжатия $\mathbf{c}_i$ блоками изображения следующим образом:

$$d_{ij} = \mathrm{dist}(\mathbf{c}_i, \mathbf{a}_i^j).$$

Для минимизации вносимых искажений при кодовом сжатии можно оптимизировать (например, минимизировать) данное расстояние при определении параметров процедуры сжатия.

Для изображения величина вносимых искажений может быть оценена следующим образом:

$$\rho = \frac{R}{\sum\limits_{i,j} d_{ij}},$$

где R — коэффициент, определяющий общие характеристики изображения.

Для изображений в качестве меры вносимых искажений ρ может быть использована хорошо известная мера $PSNR$ — пиковое отношение сигнал/шум:

$$PSNR = 20\log_{10}\frac{\max\limits_i |P_i|}{RMSE},$$

где $RMSE = \sqrt{MSE}$, $MSE = \frac{1}{L}\sum_{i=1}^{L}(P_i - Q_i)^2$, L — общее число пикселей исходного изображения, P_i, Q_i — значения i-го пикселя исходного и восстановленного изображения соответственно.

Для изображения, состоящего из пикселей по n бит каждый, величина значения функции максимума определяется как

$$\max_i |P_i| = 2^n - 1.$$

Метрика *PSNR* хорошо согласуется со свойствами зрительной системы человека, а ее максимизация позволяет получать наименее заметные искажения для изображений. Известно, что приемлемое качество восстановленных изображений возможно получить при значениях $PSNR \geq 30$ дБ.

При использовании кодового квантования для сжатия изображений в качестве метрики искажений помимо расстояния *RMSE* могут использоваться и другие метрики [7]. Например, можно использовать расстояние Хэмминга между двумя векторами: вектором, соответствующим блоку исходного изображения $\mathbf{a}_i^j$, и вектором, соответствующим блоку результирующего изображения $\mathbf{c}_i$:

$$d_H(\mathbf{a}_i^j, \mathbf{c}_i) = number \quad of \ (l : a_{il}^j \neq c_{il},\ l = 1,\ \ldots,\ K),$$

где $\mathbf{c}_i = (c_{i1}, c_{i2}, \ldots, c_{iK})$ — блок результирующего изображения с ошибкой; $\mathbf{a}_i^j = (a_{i1}^j, a_{i2}^j, \ldots, a_{iK}^j)$ — j-й блок исходного изображения. Тогда

$$\rho = \frac{R}{\sum_{i,j} d_H(\mathbf{a}_i^j, \mathbf{c}_i)},$$

где величина коэффициента R может быть выбрана специальным образом для данной метрики, например: $R = \max_{i,j} wt_H(\mathbf{a}_i^j)$.

Данная метрика хорошо согласуется с числом вносимых в процессе сжатия (кодового квантования) ошибок. Максимизация ρ, так же как и в случае с метрикой *PSNR*, приводит к минимизации числа вносимых в процессе сжатия ошибок.

Для выбранного подхода к сжатию на базе кодового квантования с использованием помехоустойчивых кодов достаточно просто реализовать процедуру кодирования, а именно функцию кодирования в процедуре сжатия F_1 с использованием метрики Хэмминга. В этом случае блок исходного изображения $\mathbf{a}_i^j$ представляется вектором длины K, подвергающимся искажениям в процессе передачи по каналу связи с ошибками. Таким образом, для исправления ошибок необходимо найти ближайшее в метрике Хэмминга кодовое слово c_i некоторого, заранее определенного, кода C. В этом случае величина искажений ρ определяется радиусом покрытия кода C, выбранного для сжатия данного изображения.

Радиус покрытия $R(C)$ линейного кода C с длиной n определяется как

$$R(C) = \max\left\{\min\left\{d_H(x, c),\ c \in C\right\},\ x \in F_2^n\right\}.$$

Соотношение между коэффициентом сжатия Θ, длиной кодового слова λ и числом информационных символов μ в выбранном помехоустойчивом коде C определяется следующим образом: $\Theta = \frac{\lambda}{\mu}$.

Для осуществления сжатия с минимальными искажениями оптимальным будет тот помехоустойчивый код, у которого радиус покрытия $R(C)$ является минимальным. Таким образом, для выполнения процедуры сжатия с заданным параметром Θ оптимальным помехоустойчивым кодом будет являться совершенный код. Однако множество линейных совершенных кодов, исправляющих ошибки, исчерпывается кодами Хэмминга и Голея [8]. Использование других кодов, исправляющих ошибки, таких как Боуза — Чоудхури — Хоквингема, Гоппы, Рида — Соломона, не оптимально и требует выполнения процедуры нахождения радиуса покрытия для каждого кода с заданными параметрами λ и μ для нахождения подходящего кода. При этом для большинства классов кодов, исправляющих ошибки, известны только нижняя и верхняя границы радиуса покрытия. Кроме того, процедура декодирования для таких кодов с исправлением числа ошибок, превосходящего половину минимального расстояния, является весьма трудоемкой задачей, в большинстве случаев требующей перебора большого числа вариантов [9].

Следует обратить внимание, что стандартный вариант функции отображения F_1 не учитывает различную значимость по восприятию искажений в изображении для элементов a_{il}^j, $l = 1, \ldots, K$ блока исходного изображения. В то же время хорошо известно, что ошибки в битах изображения, относящихся к более старшим битовым плоскостям, оказывают больше влияния на уровень искажений результирующего изображения, чем ошибки в младших битовых плоскостях. Данную особенность можно использовать при построении системы кодового сжатия.

Для разработки процедуры отображения, учитывающей различную значимость элементов изображения (взвешенную модель изображения), в работе [6] предлагается рассматривать компоненты с различными уровнями надежности в процедуре мягкого декодирования LDPC-кодов. В работах [10, 11] также предложен метод, использующий различную значимость элементов изображения при сопоставлении различным

частям кодового слова различных весов исходя из модели взвешенной структуры изображения. Результатом такого подхода явилось использование конструкции на основе кодов, исправляющих ошибки, совершенных во взвешенной метрике Хэмминга, и имеющих соответствующие параметры. Схожий подход, основанный на использовании различной значимости элементов изображения и применении LEBC-кодов, был рассмотрен в работах [12–15]. В работе [15] приведено сравнение различных методов, использующих различную значимость элементов изображения и взвешенную метрику.

Основным достоинством первого подхода является использование механизма, позволяющего адаптироваться к значимости элементов изображения (битов на определенных битовых плоскостях) для каждого блока исходного изображения. То есть предлагается исправлять ошибки, вносимые в процессе выполнения алгоритма декодирования, учитывая ошибки, внесенные на предыдущих шагах алгоритма. С другой стороны, такая процедура сжатия имеет существенный недостаток, так как требует больших вычислительных затрат при обработке блоков исходного изображения. Вторым ограничением данного подхода является слишком грубая оценка общего числа искажений, вносимых в процессе кодового квантования исходного блока изображения. Для оценки таких искажений можно использовать границы радиуса покрытия для применяемого класса кодов, исправляющих ошибки [16], или точное значение радиуса покрытия для кода с заданной порождающей матрицей, вычисление которого в общем случае является трудоемкой задачей.

Основным преимуществом второго подхода является гарантия максимально возможной величины общего числа взвешенных искажений, приходящихся на блок исходного изображения, которая будет не более чем некоторое пороговое значение, равное радиусу покрытия кода. Кроме того, величина радиуса покрытия связана с радиусом сферической упаковки и для совершенного кода равна половине минимального расстояния. Следовательно, для его определения не требуется каких-либо сложных и трудоемких вычислений.

Таким образом, для осуществления сжатия будем использовать конструкции на основе помехоустойчивых кодов, совершенных во взвешенной метрике Хэмминга.

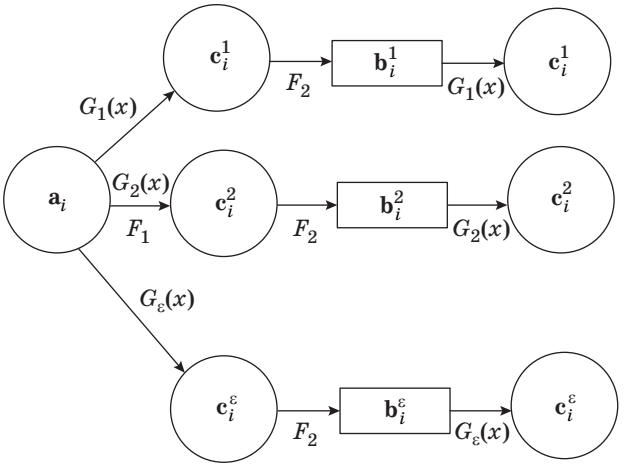
Совместное маскирование и сжатие изображения с использованием помехоустойчивых кодов

Для выбранного подхода возможна реализация в процессе кодового сжатия еще и процедуры маскирования изображения. Для этого рассмотрим процедуру сжатия, использующую на первом шаге различные коды Гоппы $\{C_1, C_2, ..., C_\varepsilon\}$, определенные их многочленами Гоппы $\{G_1(x), G_2(x), ..., G_\varepsilon(x)\}$. В общем случае получаем различные кодовые слова для одного и того же блока исходного изображения (рис. 3).

В работе [17], где подробно описан вариант реализации первого шага сжатия (функция F_1), предлагалось использовать коды Гоппы, совершенные во взвешенной метрике Хэмминга, для задач защиты авторских прав на изображения. В работах [17, 18] был предложен алгоритм маскирования изображений с использованием кодов Гоппы. Настоящая работа является дальнейшим развитием и агрегацией идей, изложенных в работах [17–19], позволяющим обеспечить одновременное сжатие и маскирование исходного изображения с использованием кодов Гоппы, совершенных во взвешенной метрике Хэмминга.

Рассмотрим в качестве примера простейший случай, при котором возьмем два кода Гоппы, совершенных во взвешенной метрике Хэмминга, для блока исходного изображения **b**, состоящего из 8 пикселей, каждый из которых представлен восьмью битами. Таким образом, $m = 8$, $n = 8$, $K = 64$.

Для сжатия данного блока будем использовать два различных кода Гоппы C_1 и C_2 со следующими параметрами: $\lambda_1 = 35$, $\mu_1 = 29$, при этом $\lambda_{11} = 8$, $\lambda_{12} = 27$ (где λ_{11} — часть блока исходного изображения, имеющая меньшую значимость, чем часть блока, соответствующая λ_{12}), с $\deg G_1(x) = 2$ и $\lambda_2 = 29$, $\mu_2 = 23$ при $\lambda_{21} = 4$, $\lambda_{22} = 6$, $\lambda_{23} = 19$ (где λ_{21} — часть блока исходного изображения, имеющая меньшую значимость, чем часть блока,



■ ***Рис. 3.*** Отображение блока исходного изображения при использовании различных кодов Гоппы

■ ***Fig. 3.*** Initial block to resulting compressed block mapping based on different Goppa codes

соответствующая λ_{22} и λ_{23}, а λ_{22} — меньшую, чем λ_{23}) с $\deg G_2(x) = 3$ соответственно. $G_1(x)$ и $G_2(x)$ — неприводимые многочлены с коэффициентами их $GF(2^2)$ и $GF(2^3)$ соответственно. Общее число информационных символов для этой пары кодов $k = \mu_1 + \mu_2 = 29 + 23 = 51$. Таким образом, коэффициент сжатия для данного примера $\Theta = 64/51 = 1{,}25$.

Далее для выбранного примера разобьем блок исходного изображения на три подблока с длинами $K_1 = \lambda_{11} + \lambda_{21} = 12$, $K_2 = \lambda_{12} + \lambda_{22} = 33$, $K_3 = \lambda_{23} = 19$. Веса блоков, отражающие влияние возникающей ошибки на результирующие искажения, определим как $\upsilon_1 = 1$, $\upsilon_2 = 2$, $\upsilon_3 = 3$ соответственно. Таким образом, чем больше вес подблока, тем больше влияние происходящих в нем ошибок на результирующие искажения в изображении.

Оба кода в примере являются совершенными во взвешенной метрике Хэмминга, и радиус покрытия для приведенных кодов определяется как

$$R(C_1) = \max_{\upsilon_1 t_1 + \upsilon_2 t_2 \le \deg G_1(x)} t_1 + t_2 = 2;$$

$$R(C_2) = \max_{\upsilon_1 t_1 + \upsilon_2 t_2 + \upsilon_3 t_3 \le \deg G_2(x)} t_1 + t_2 + t_3 = 3.$$

Структура корректирующей способности этих кодов может быть представлена в табл. 1 и 2.

В приведенных таблицах t_1 и t_2 — число ошибок в подблоках кодового слова кода C_1 длины $\lambda_{11} = 8$, $\lambda_{12} = 27$ соответственно. Из табл. 1 видно, что если в менее значимом подблоке λ_{11} произойдет одна или две ошибки, то в более значимом подблоке λ_{12} может произойти 0 ошибок (второй и третий столбцы таблицы), т. е. ошибок во втором более значимом подблоке произойти не может. В то же время если ошибка произойдет во втором подблоке, то ни одной ошибки в менее значимом подблоке произойти не может. При этом максимально возможное число ошибок для подблока λ_{11} равно 2, а для подблока λ_{12} равно 1. В процессе сжатия может происходить меньшее число ошибок, но не большее. В табл. 2 приведено распределение ошибок для кода C_2 при условии наличия трех подблоков. Смысл приведенных значений интерпретируется так же, как и для табл. 1.

Для того чтобы сжать блок исходного изображения, необходимо покрыть его кодовыми словами определенных выше двух кодов Гоппы C_1 и C_2. Один из возможных вариантов разбиения блока исходного изображения на кодовые слова первого и второго кодов Гоппы с учетом взвешенной структуры изображения приведен на рис. 4.

Проанализируем распределение ошибок для приведенного примера. Обозначим под единым вектором $\mathbf{l}_{678}$ множество трех векторов наиболее значащих бит изображения, обозначенных как MSB, 7LSB и 6LSB. Данный вектор состоит из 24 бит. Множество бит, состоящее из векторов 5LSB и 4LSB, обозначим как вектор $\mathbf{l}_{45}$, состоящий из 16 бит. Аналогично получим векторы $\mathbf{l}_3$ (3LSB), $\mathbf{l}_2$ (2LSB) и $\mathbf{l}_1$ (LSB — наименее значимые биты), состоящие из 8 бит каждый. Таким образом, получаем следующую структуру блока **b**:

$$\mathbf{b} = (\mathbf{l}_{678}, \mathbf{l}_{45}, \mathbf{l}_3, \mathbf{l}_2, \mathbf{l}_1).$$

Для данного вектора выпишем таблицу со значениями возможного максимального числа

■ ***Таблица 1***. Возможное распределение ошибок в подблоке для кода C_1

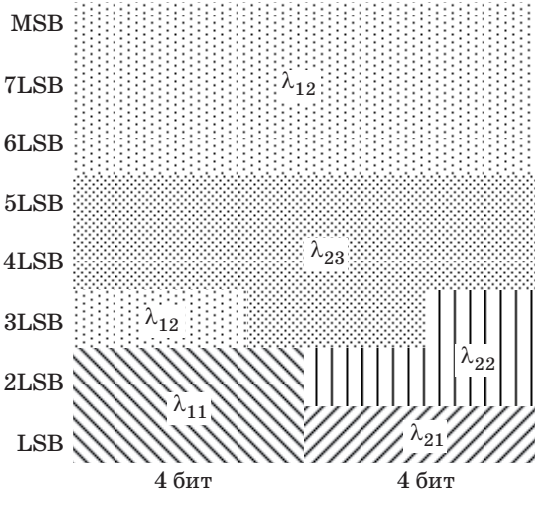
■ ***Table 1***. Possible error distribution in the sub block for error-correcting code C_1

Вес ошибки	Число ошибок	Варианты распределения ошибок по блокам кода C_1			
$\upsilon_2 = 2$	t_2	0	0	0	1
$\upsilon_1 = 1$	t_1	0	1	2	0

■ ***Таблица 2***. Возможное распределение ошибок в подблоке для кода C_2

■ ***Table 2***. Possible error distribution in the sub block for error-correcting code C_2

Вес ошибки	Число ошибок	Варианты распределения ошибок по блокам кода C_2						
$\upsilon_3 = 3$	t_3	0	0	0	0	0	0	1
$\upsilon_2 = 2$	t_2	0	0	0	0	1	1	0
$\upsilon_1 = 1$	t_1	0	1	2	3	0	1	0



■ ***Рис. 4***. Вариант разбиения блока **b** исходного изображения на кодовые слова первого и второго кодов Гоппы

■ ***Fig. 4***. The variant of block **b** dividing on codewords of first and second Goppa codes

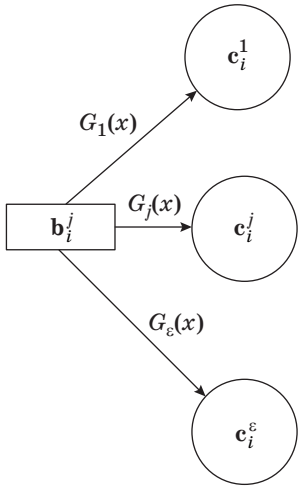
суммарных ошибок, распределенных по векторам $\mathbf{l}_{678}$, $\mathbf{l}_{45}$, $\mathbf{l}_3$, $\mathbf{l}_2$, $\mathbf{l}_1$, для показанной на рис. 4 структуры. Найденное распределение приведено в табл. 3.

В таблице приведены наихудшие варианты возникновения ошибок в процессе сжатия для выбранных кодов и для выбранного распределения кодовых слов в сжимаемом блоке. Для реальных изображений распределение ошибок может оказаться существенно лучше, но не хуже.

Проанализируем возможности шифрования полученной структуры для выбранного примера. Обозначим как S_1 и S_2 число различных неприводимых многочленов $G_1(x)$ и $G_2(x)$, определяющих различные коды Гоппы с параметрами $\lambda_1 = 35$, $\mu_1 = 29$ и $\lambda_2 = 29$, $\mu_2 = 23$. Тогда $S_1 = 28$, $S_2 = 20$.

Поскольку в результате выполнения функции сжатия F_1 каждый блок изображения может быть ассоциирован с одной из 560 пар для выбранных в примере параметров, принадлежащих кодам Гоппы с многочленами $G_1(x)$ и $G_2(x)$, то множество таких пар можно использовать в качестве ключа шифрования и дешифрования. Если в процессе дешифрации (декомпрессии) будет использоваться другая пара кодов (иные многочлены Гоппы), чем те, которые использовались при сжатии, то результатом окажется иной блок изображения, так как он будет кодовым словом другого кода Гоппы. Данная ситуация представлена на рис. 5.

Результатом такой неправильной декомпрессии станет появление дополнительных ошибок, что в значительной степени может ухудшить качество восстановленного после сжатия изображения.



■ ***Рис. 5.*** Декомпрессия изображения при использовании различных многочленов Гоппы в качестве ключа дешифрации

■ ***Fig. 5.*** Image decompression by using different Goppa polynomials as a secret key

■ ***Таблица 3.*** Распределение максимально возможного числа суммарных ошибок по векторам $\mathbf{l}_{678}$, $\mathbf{l}_{45}$, $\mathbf{l}_3$, $\mathbf{l}_2$, $\mathbf{l}_1$ для кодов C_1 и C_2

■ ***Table 3.*** Possible $\mathbf{l}_{678}$, $\mathbf{l}_{45}$, $\mathbf{l}_3$, $\mathbf{l}_2$, $\mathbf{l}_1$ variance of maximum summarize error appearance for vectors for error-correcting codes C_1 and C_2

Вектор	Варианты распределения максимальных суммарных ошибок по векторам $\mathbf{l}$													
Для кода C_1														
$\mathbf{l}_{678}$	0	1	1	0	0	0	0	0	0	0	0	0	0	0
$\mathbf{l}_{45}$	0	0	1	1	0	0	0	0	0	0	0	0	0	0
$\mathbf{l}_3$	0	0	0	0	1	1	1	1	1	1	2	1	0	0
$\mathbf{l}_2$	0	0	0	0	0	1	1	0	0	0	0	2	1	1
$\mathbf{l}_1$	0	0	0	0	0	0	1	1	2	3	0	0	0	1
Для кода C_2														
$\mathbf{l}_{678}$	0	0	0	0	0	0	0	0	0	0	0	0	0	
$\mathbf{l}_{45}$	0	0	0	0	0	0	0	0	0	0	0	0	0	
$\mathbf{l}_3$	0	0	0	0	0	0	0	0	0	0	0	0	0	
$\mathbf{l}_2$	1	1	1	2	2	2	3	3	0	0	0	0	0	
$\mathbf{l}_1$	2	3	4	1	2	3	0	1	1	2	3	4	5	

Дополнительным эффектом от применения указанного подхода является то, что в процессе кодового сжатия с шифрованием изображение автоматически покрывается кодовыми словами выбранных в качестве ключа кодов. Данное свойство может быть использовано в качестве цифрового водяного знака для защиты авторских прав на изображения [20].

Заключение

Для выполнения эффективной процедуры сжатия и маскирования при условии достижения гарантированного коэффициента сжатия и гарантированного минимального числа вносимых ошибок наиболее эффективным подходом является применение помехоустойчивых кодов. При этом применение кодов Гоппы, совершенных во взвешенной метрике Хэмминга, хорошо согласовано с особенностями такого объекта обработки, как мультимедиаданные, например изображения. Данный класс кодов позволяет при осуществлении сжатия с потерями добиваться перераспределения возникающих ошибок в соответствии со взвешенной структурой изображения, т. е. осуществить перераспределение ошибок в сторону наименее значимых бит в заданной взвешенной модели объекта сжатия. Также появляется возможность реализации параллельного маскирования сжимаемого изображения в целях его защиты. Данная возможность обусловлена использованием в качестве секретного ключа заданной комбинации многочленов Гоппы, вслед-

ствие чего при декомпрессии изображений с неверным ключом восстановленное изображение имеет неприемлемое качество. Кроме того, важным свойством предложенного метода является формирование цифрового водяного знака при выполнении процедуры совместного сжатия с маскированием, покрывающего все пространство изображения и являющегося основанием для защиты авторского права на изображение.

Данная работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований в 2017 г. (грант № 17-07-00849-А).

Литература

1. **Cintuglu M. H., Mohammed O. A., Akkaya K., and Uluagac A. S.** A Survey on Smart Grid Cyber-physical System Testbeds // IEEE Communications Surveys & Tutorials. 2017. Vol. 19. N 1. P. 446–464.
2. **Mo Y., Weerakkody S., and Sinopoli B.** Physical Authentication of Control Systems: Designing Watermarked Control Inputs to Detect Counterfeit Sensor Outputs// IEEE Control Systems. 2015. Vol. 35. N 1. P. 93–109.
3. **Sandberg H., Amin S., and Johansson K. H.** Cyber-physical Security in Networked Control Systems: An Introduction to the Issue // IEEE Control Systems. 2015. Vol. 35. N 1. P. 20–23.
4. **Hu H.-T., and Hsu L.-Y.** Collective Blind Image Watermarking in DWTDCT Domain with Adaptive Embedding Strength Governed by Quality Metrics // Multimedia Tools and Applications. 2017. Vol. 76. N 5. P. 6575–6594.
5. **Lai C.-C., and Tsai C.-C.** Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition // IEEE Transactions on Instrumentation and Measurement. 2010. Vol. 59. N 11. P. 3060–3063.
6. **Belogolovyi A.** Image Compression Based on LDPC Codes //Proc. of Intern. Conf. Graphicon, 2004. www.graphicon.ru (дата обращения: 18.09.2017).
7. **Guyeux C., and Bahi J. M.** Topological Chaos and Chaotic Iterations Application to Hash Functions // Proc. of the 2010 Intern. Joint Conf. on Neural Networks (IJCNN). 2010. P. 1–7.
8. **Bezzateev S., and Shekhunova N.** Class of Generalized Goppa Codes Perfect in Weighted Hamming Metric // Designs, Codes and Cryptography. 2013. Vol. 66. N 1–3. P. 391–399.
9. **Крук Е. А., Сергеев М. Б.** О векторном квантовании изображений // Информационно-управляющие системы. 2013. № 3. С. 93–96.
10. **Bezzateev S., Voloshina N., and Zhidanov K.** Steganographic Method on Weighted Container // Proc. of XIII Intern. Symp. on Problems of Redundancy in Information and Control Systems (RED). 2012. P. 10–12.
11. **Bezzateev S., Voloshina N., and Minchenkov V.** Special Class of (L,G) Codes for Watermark Protection in DRM // Proc. of 8th Intern. Conf. on Computer Science and Information Technologies. 2011. P. 225–228.
12. **Feng K., Xu L., Hickernell F.** Linear Error-Block Codes// Finite Fields Appl. 2006. N 6. P. 638–652.
13. **Darit R., Souidi E. M.** New Families of Perfect Linear Error-Block Codes // Intern. Journal of Information and Coding Theory (IJICOT). 2013. N 2(2/3). P. 84–95.
14. **Dariti R., Souidi E. M.** An Application of Linear Error-block Codes in Steganography // Intern. Journal of Digital Information and Wireless Communications (IJDIWC). 2011. Vol. 1. N 2. P. 426–433.
15. **Voloshina N., Bezzateev S., Zhidanov K.** Weighted Digital Watermarking Approaches Comparison // Problems of Redundancy in Information and Control Systems: XV Intern. Symp., Saint-Petersburg, September 26–29, 2016. P. 172–174.
16. **Bezzateev S., Shekhunova N.** Lower Bound of Covering Radius of Binary Irreducible Goppa Codes // Designs, Codes and Cryptography. 2017. Vol. 82. Iss. 1. P. 69–76.
17. **Беззатеев С. В., Волошина Н. В., Жиданов К. А.** Система формирования фингерпринта статических изображений с использованием взвешенной метрики Хэмминга и модели взвешенного контейнера // Докл. Томского государственного университета систем управления и радиоэлектроники. 2014. № 2(32). С. 246–251.
18. **Беззатеев С. В., Литвинов М. Ю., Трояновский Б. К., Филатов Г. П.** Выбор алгоритма преобразования, обеспечивающего изменение структуры изображения // Информационно-управляющие системы. 2006. № 6. С. 2–6.
19. **Беззатеев С. В., Литвинов М. Ю., Трояновский Б. К.** Использование помехоустойчивых кодов для шифрации видеоинформации // Информационно-управляющие системы. 2007. № 5. С. 23–26.
20. **Bezzateev S., and Voloshina N.** Digital Watermarking Method Based on Image Compression Algorithms // Internet of Things, Smart Spaces, and Next Generation Networks and Systems. 2017. P. 292–299.

UDC 681.3, 004.932.2
doi:10.15217/issn1684-8853.2017.6.88

Masking Compression based on Weighted Image Structure Model

Bezzateev S. V.[a], Dr. Sc., Tech., Associate Professor, bsv@aanet.ru
Voloshina N. V.[a], PhD, Tech., Associate Professor, nataliv@yandex.ru
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: To organize efficient and safe storage and transmission of video information, two independent sequential procedures are necessary: compression and masking. To get the initial image at the receiver's end, the operations of decompression and decryption should be performed in the reverse order. For decompression, you need to have so-called "code book" which is similar to a key in encryption and decryption. **Purpose:** An efficient way to combine the procedures of compression and masking for digital images. **Results:** A compression method is proposed which takes into account the significance of various parts of the original multimedia object (image) to improve the quality of the resulting image after the decompression. One of the most effective approaches to solve this problem is using Error Correcting Codes, thus limiting the number of compression errors (distortions) and ensuring the required value of the compression ratio. The use of such codes for compression makes it possible to distribute the errors added during the processing in accordance with the predefined significance of the original multimedia object elements. As an example, we present an approach based on the weighted Hamming metric which allows you to ensure a predefined maximum number of errors (distortions) and takes into account the predefined significance of image zones (weighted image structure). To implement the proposed method of combined masking and compression, we chose a subclass of Goppa codes which are perfect in a weighted Hamming metric. Goppa polynomials were used as a secret key. The result of using the proposed method was covering the entire image with a unique digital watermark. **Practical relevance:** The proposed approach can be applied in systems with increased quality demands concerning the stored and transmitted images when using open transmission channels. It will provide a guaranteed compression effect at a given level of the introduced distortions and a high level of information protection.

Keywords — Compression Based on Codes, Perfect Codes, Weighted Distance Metric, Steganography.

References

1. Cintuglu M. H., Mohammed O. A., Akkaya K., and Uluagac A. S. A Survey on Smart Grid Cyber-physical System Testbeds. *IEEE Communications Surveys & Tutorials*, 2017, vol. 19, no. 1, pp. 446–464.
2. Mo Y., Weerakkody S., and Sinopoli B. Physical Authentication of Control Systems: Designing Watermarked Control Inputs to Detect Counterfeit Sensor Outputs. *IEEE Control Systems*, 2015, vol. 35, no. 1, pp. 93–109.
3. Sandberg H., Amin S., and Johansson K. H. Cyberphysical Security in Networked Control Systems: An Introduction to the Issue. *IEEE Control Systems*, 2015, vol. 35, no. 1, pp. 20–23.
4. Hu H.-T., and Hsu L.-Y. Collective Blind Image Watermarking in DWTDCT Domain with Adaptive Embedding Strength Governed by Quality Metrics, *Multimedia Tools and Applications*, 2017, vol. 76, no. 5, pp. 6575– 6594.
5. Lai C.-C. and Tsai C.-C. Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition. *IEEE Transactions on Instrumentation and Measurement*, 2010, vol. 59, no. 11, pp. 3060–3063.
6. Belogolovyi A. Image Compression based on LDPC Codes. *Proc. of Intern. Conf. Graphicon*, 2004. Available at: www.graphicon.ru (accessed 18 September 2017).
7. Guyeux C., and Bahi J. M. Topological Chaos and Chaotic Iterations Application to Hash Functions. *Proc. of the 2010 Intern. Joint Conf. on Neural Networks (IJCNN)*, 2010, pp. 1–7.
8. Bezzateev S., and Shekhunova N. Class of Generalized Goppa Codes Perfect in Weighted Hamming Metric. *Designs, Codes and Cryptography*, 2013, vol. 66, no. 1-3, pp. 391–399.
9. Krouk E. A., Sergeev M. B. Vector Quantization of Images. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2013, no. 3, pp. 93–96 (In Russian).
10. Bezzateev S., Voloshina N., and Zhidanov K. Steganographic Method on Weighted Container. *Proc. of XIII Intern. Symp. on Problems of Redundancy in Information and Control Systems (RED)*, 2012, pp. 10–12.
11. Bezzateev S., Voloshina N., and Minchenkov V. Special Class of (L,G) Codes for Watermark Protection in DRM. *Proc. of 8th Intern. Conf. on Computer Science and Information Technologies*, 2011, pp. 225–228.
12. Feng K., Xu L., Hickernell F. Linear Error-Block Codes. *Finite Fields Appl.*, 2006, no. 6, pp. 638–652.
13. Darit R., Souidi E. M. New Families of Perfect Linear Error-Block Codes. *Intern. Journal of Information and Coding Theory (IJICOT)*, 2013, no. 2(2/3), pp. 84–95.
14. Dariti R., Souidi E. M. An Application of Linear Error-block Codes in Steganography. *Intern. Journal of Digital Information and Wireless Communications (IJDIWC)*, 2011, vol. 1, no. 2, pp. 426–433.
15. Voloshina N., Bezzateev S., Zhidanov K. Weighted Digital Watermarking Approaches Comparison. *Proc. of XV Intern. Symp. "Problems of Redundancy in Information and Control Systems"*, Saint-Petersburg, September 26–29, 2016, pp. 172–174.
16. Bezzateev S., Shekhunova N. Lower Bound of Covering Radius of Binary Irreducible Goppa Codes. *Designs, Codes and Cryptography*, 2017, vol. 82, no. 1, pp. 69–76.
17. Bezzateev S. V., Voloshina N. V., Zhidanov K. A. The Method of Digital Fingerprinting for Static Images Based on Weighted Hamming Metric and on Weighted Container Model. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniia i radioelektroniki* [Proc. of TUSUR], 2014, no. 2, pp. 246–251 (In Russian).
18. Bezzateev S. V., Litvinov M. Y., Troyanovskii B. K., Filatov G. P. The Choice of the Transformation Algorithm that Ensures a Structural Change of Videoinformation. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2006, no. 6, pp. 2–6 (In Russian).
19. Bezzateev S. V., Litvinov M. Y., Troyanovskii B. K. Using Error-Correcting Codes for Video Information Encoding. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2007, no. 5, pp. 23–26 (In Russian).
20. Bezzateev S., and Voloshina N. Digital Watermarking Method based on Image Compression Algorithms. In: *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, 2017, pp. 292–299.